UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,062	12/30/2003	Daryl Carvis Cromer	RPS20030216US1	8316

36491 7590 06/12/2007

Kunzler & McKenzie
8 EAST BROADWAY
SUITE 600
SALT LAKE CITY, UT 84111

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	

MAIL DATE	DELIVERY MODE
06/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/748,062	CROMER ET AL.	
	Examiner	Art Unit	
	Ellen C. Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Ellen Tran

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *30 Dec '03*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is responsive to: amendment filed original application filed on 30 December 2003..

2. Claims 1-30 are pending; claims 1, 7, 13, 17, 22, and 27, are independent claims.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. **Claims 1-3,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Ripley U.S. Patent No. 7,111,175 (hereinafter Ripley) in view of Wiseman et al. U.S. Patent No. 7,216,369 (hereinafter Wiseman).

As to independent claim 1, "An apparatus for secure computer readable medium backup, the apparatus comprising: a computer readable medium having at least a first accessible portion and a second encrypted portion"; is taught in Ripley col. 4, lines 4-46; the following is not explicitly taught in Ripley: **"and a trusted platform interface module operatively coupled with the computer readable medium and configured to communicate with a cryptographic module"** however Wiseman teaches a Trusted Computing Platform Alliance (TCPA) that contains a platform, a security module, and a storage device in col. 5, lines 8-31.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and apparatus for verifying the integrity of a media key block taught in Ripley to include a means insure the interface modules are a trusted platform. One of ordinary skill in the art would have been motivated to perform such a modification because of the need for data security see Wiseman (col. 1, lines 24 et seq.) "In a world increasingly influenced by the existence of networks connecting a widespread array of computing resources, the topics of data security, information protection, and user privacy have never been more important. Personal computers (PCs) typically offer an open architecture as an industry standard which can be used to build a ubiquitous computing platform. Trust in the platform, however, has not commonly been part of such designs. As used herein, the term "platform" can be taken to mean any type of device, including hardware, firmware, software, or any combination of these, whose activity is directed according to a plurality of programmed instructions".

As to dependent claim 2, "wherein the cryptographic module comprises a trusted platform module (TPM)" however Wiseman teaches a security module the security module is a TPM see col. 5, lines 6-21. The motivation to combine Ripley and Wiseman is the same as stated above in claim 1.

As to dependent claim 3, "wherein the computer readable medium comprises a computer readable peripheral selected from the group consisting of a hard disk drive, a universal serial bus storage device, a floppy disk, an optical storage disk, a flash memory storage device, and a network attached storage drive" is taught in Ripley col. 4, lines 36-46.

5. **Claims 4 and 5,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Ripley U.S. Patent No. 7,111,175 (hereinafter Ripley) in view of Wiseman et al. U.S. Patent No.

7,216,369 (hereinafter Wiseman) in further view of Yoshino et al. U.S. Patent No. 7,124,317 (hereinafter Yoshino).

As to dependent claim 4, the following is not explicitly taught in the combination of Ripley and Wiseman: **"wherein the trusted platform interface module further comprises a password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module"** however Yoshino teaches the exchange of encrypted keys for authentication between media and the device it is loaded into in col. 34, lines 42-57. Note the Examiner interprets the exchanged key equivalent to passwords.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and apparatus for verifying the integrity of a media key block with a trusted module interface taught in Ripley and Wiseman to include a means to transmit encrypted passwords. One of ordinary skill in the art would have been motivated to perform such a modification because a needs exists for assurance of security without increasing processor load see Yoshino (col. 2, lines 42 et seq.) "It is an object of the present invention to provide an information recording device, an information playback device, and an information playback method in which, in the construction of storing data in units of sectors, ICVs are set in units of sectors, without increasing a processing load on a device side. It is also an object of the present invention to provide an information recording medium and a program providing medium which are used therewith".

As to dependent claim 5, "wherein the encrypted password comprises a unique password configured to be decrypted by the cryptographic module that first created the

encrypted password" however Yoshino col. 34, lines 42-67 teach mutual authentication by the exchange of encrypted keys, it is obvious that the agreed session key is created by the was created on the device the media was loaded. The motivation to combine Ripley, '389, and Yoshino is the same as stated above in claim 4.

6. **Claim 6,** is rejected under 35 U.S.C. 103(a) as being unpatentable over of Ripley U.S. Patent No. 7,111,175 (hereinafter Ripley) in view of Wiseman et al. U.S. Patent No. 7,216,369 (hereinafter Wiseman) in further view of Second Copy 2000, software release noted November, 1999 (hereinafter Second Copy 2000).

As to dependent claim 6, the following is not explicitly taught in the combination of Ripley and Wiseman: **"wherein the computer readable medium module further comprises a backup utility module configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium with newer versions of the data"** however Second Copy 2000 teaches that new versions can be maintained on page 3, paragraph 2.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and apparatus for verifying the integrity of a media key block with a trusted module interface taught in Ripley and Wiseman to include a means for a backup utility to selectively copy data from a storage device based on the version of data stored. One of ordinary skill in the art would have been motivated to perform such a modification because a needs exists to improve the amount of processor time and storage space needed while performing backups see Second Copy 2000 (page 3, 3rd paragraph) "Running in the background, Second Copy doesn't waste your

valuable time. And, designed to back up only those files that have been updated since your last backup, Second Copy doesn't waste your computer's time".

7. **Claims 7, 11, and 12,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Nonaka et al. U.S. Patent Publication No. 2001/0003517 (hereinafter Nonaka) in view of Yoshino et al. U.S. Patent No. 7,124,317 (hereinafter Yoshino).

As to independent claim 7, "A device for secure computer readable medium backup, the device comprising: a motherboard" is taught in Nonaka page 2, paragraphs 0020-0021; the following is not explicitly taught in Nonaka: **"and a cryptographic module coupled to the motherboard and configured to communicate with a computer readable medium"** however Yoshino teaches the memory interface unit includes a cryptosystem unit in col. 2, lines 51-65.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and system for recording and reproducing information taught in Nonaka to include a means to utilize a cryptographic module. One of ordinary skill in the art would have been motivated to perform such a modification because a needs exists for assurance of security without increasing processor load see Yoshino (col. 2, lines 42 et seq.) "It is an object of the present invention to provide an information recording device, an information playback device, and an information playback method in which, in the construction of storing data in units of sectors, ICVs are set in units of sectors, without increasing a processing load on a device side. It is also an object of the present invention to provide an information recording medium and a program providing medium which are used therewith".

As to dependent claim 11, "wherein the motherboard further comprises a memory, and a processor coupled to the memory" is taught in Nonaka page 2, paragraph 0020-0021.

As to dependent claim 12, "wherein the computer readable medium comprises a computer readable peripheral selected from the group consisting of a hard disk drive, a universal serial bus storage device, a floppy disk, an optical storage disk, a flash memory storage device, and a network attached storage drive" is shown in Nonaka page 2, paragraphs 0022-0023.

8. **Claims 8-10,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Nonaka et al. U.S. Patent Publication No. 2001/0003517 (hereinafter Nonaka) in view of Yoshino et al. U.S. Patent No. 7,124,317 (hereinafter Yoshino) in further view of Wiseman et al. U.S. Patent No. 7,216,369 (hereinafter Wiseman).

As to dependent claim 8, the following is not explicitly taught in the combination of Nonaka and Yoshino: **"wherein the computer readable medium further comprises a trusted platform interface module configured to communicate with the cryptographic module and transmit an encrypted password"** however '389 teaches a Trusted Computing Platform Alliance (TCPA) that contains a platform, a security module, and a storage device in col. 5, lines 8-31.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and apparatus for verifying the integrity of a media key block with a cryptographic module taught in Ripley and Yoshino to include a means insure the interface modules are a trusted platform. One of ordinary skill in the art would have been motivated to perform such a modification because of the need for data security see Wiseman (col. 1, lines 24 et seq.) "In a

world increasingly influenced by the existence of networks connecting a widespread array of computing resources, the topics of data security, information protection, and user privacy have never been more important. Personal computers (PCs) typically offer an open architecture as an industry standard which can be used to build a ubiquitous computing platform. Trust in the platform, however, has not commonly been part of such designs. As used herein, the term "platform" can be taken to mean any type of device, including hardware, firmware, software, or any combination of these, whose activity is directed according to a plurality of programmed instructions".

As to dependent claim 9, "wherein the cryptographic module is configured to receive the encrypted password from trusted platform interface module, decrypt the password, and transmit the decrypted password to the trusted platform interface module" however Yoshino teaches the exchange of encrypted keys for authentication between media and the device it is loaded into in col. 34, lines 42-57. The motivation to combine Nonaka, Yoshino, and Wiseman is the same as stated above in claim 8.

As to dependent claim 10, "wherein the cryptographic module comprises a trusted platform module (TPM)" however '389 teaches a Trusted Computing Platform Alliance (TCPA) that contains a platform, a security module, and a storage device in col. 5, lines 8-31. The motivation to combine Nonaka, Yoshino, and Wiseman is the same as stated above in claim 8.

9. **Claims 13-15,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Nonaka et al. U.S. Patent Publication No. 2001/0003517 (hereinafter Nonaka) in view of Yoshino et al.

U.S. Patent No. 7,124,317 (hereinafter Yoshino) in further view of Wiseman et al. U.S. Patent No. 7,216,369 (hereinafter Wiseman).

As to independent claim 13, "A system for secure computer readable medium backup, the system comprising: a motherboard" is taught in Nonaka page 2, paragraphs 0020-0021;

the following is not explicitly taught in Nonaka:

"a cryptographic module coupled to the motherboard configured to decrypt encrypted passwords" however Yoshino teaches the exchange of encrypted keys for authentication between media and the device it is loaded into in col. 34, lines 42-57;

"a computer readable medium module having at least a first accessible portion and a second encrypted portion" however Yoshino teaches that an Encryption Flag indicates whether a sector in encrypted or non-encrypted in col. 15, lines 33-38;

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and system for recording and reproducing information taught in Nonaka to include a means to utilize a cryptographic module. One of ordinary skill in the art would have been motivated to perform such a modification because a needs exists for assurance of security without increasing processor load see Yoshino (col. 2, lines 42 et seq.) "It is an object of the present invention to provide an information recording device, an information playback device, and an information playback method in which, in the construction of storing data in units of sectors, ICVs are set in units of sectors, without increasing a processing load on a device side. It is also an object of the present invention to provide an information recording medium and a program providing medium which are used therewith".

the following is not explicitly taught in the combination of Nonaka and Yoshino: **"and a trusted platform interface module operatively coupled with the computer readable media module and configured to communicate with a cryptographic module"** however Wiseman teaches a Trusted Computing Platform Alliance (TCPA) that contains a platform, a security module, and a storage device in col. 5, lines 8-31.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and system for recording and reproducing information that utilizes a cryptographic module taught in Nonaka and Yoshino to include a means insure the interface modules are a trusted platform. One of ordinary skill in the art would have been motivated to perform such a modification because of the need for data security see Wiseman (col. 1, lines 24 et seq.) "In a world increasingly influenced by the existence of networks connecting a widespread array of computing resources, the topics of data security, information protection, and user privacy have never been more important. Personal computers (PCs) typically offer an open architecture as an industry standard which can be used to build a ubiquitous computing platform. Trust in the platform, however, has not commonly been part of such designs. As used herein, the term "platform" can be taken to mean any type of device, including hardware, firmware, software, or any combination of these, whose activity is directed according to a plurality of programmed instructions".

As to dependent claims 14, "further comprising a password module configured to store and transmit an encrypted password to the cryptographic module, and receive an unencrypted password from the cryptographic module" however Yoshino teaches the exchange of encrypted keys for authentication between media and the device it is loaded into in

col. 34, lines 42-57. Note the Examiner interprets the exchanged key equivalent to passwords. The motivation to combine Nonaka, Yoshino, and Wiseman is the same as stated above in claim 13.

As to dependent claims 15 "wherein the encrypted password is configured to be decrypted by the cryptographic module that first created the encrypted password" however Yoshino col. 34, lines 42-67 teach mutual authentication by the exchange of encrypted keys, it is obvious that the agreed session key is created by the was created on the device the media was loaded. The motivation to combine Nonaka, Yoshino, and Wiseman is the same as stated above in claim 13.

10. **Claim 16,** is rejected under 35 U.S.C. 103(a) as being unpatentable over of Nonaka et al. U.S. Patent Publication No. 2001/0003517 (hereinafter Nonaka) in view of Yoshino et al. U.S. Patent No. 7,124,317 (hereinafter Yoshino) in further view of Wiseman et al. U.S. Patent No. 7,216,369 (hereinafter Wiseman) in further view of Second Copy 2000, software release noted November, 1999 (hereinafter Second Copy 2000).

As to dependent claims 16, the following is not explicitly taught in the combination of Nonaka, 317, and Wiseman: **"wherein the computer readable medium further comprises a backup utility configured to selectively copy data from a storage device source, detect newer versions of data stored on the storage device source, and replace older versions of the data on the computer readable medium module with newer versions of the data"** however Second Copy 2000 teaches that new versions can be maintained on page 3, paragraph 2 and that older backup can be deleted.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and system for recording and reproducing information that utilizes a cryptographic module and trusted platform modules taught in Nonaka, 317, and Wiseman to include a means for a backup utility to selectively copy data from a storage device based on the version of data stored. One of ordinary skill in the art would have been motivated to perform such a modification because a needs exists to improve the amount of processor time and storage space needed while performing backups see Second Copy 2000 (page 3, 3rd paragraph) "Running in the background, Second Copy doesn't waste your valuable time. And, designed to back up only those files that have been updated since your last backup, Second Copy doesn't waste your computer's time".

11. **Claims 17, 18, 20-23, 25-28, and 30,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Ripley U.S. Patent No. 7,111,175 (hereinafter Ripley) in view of Yoshino et al. U.S. Patent No. 7,124,317 (hereinafter Yoshino).

As to independent claim 22, "A method for secure computer readable medium backup, the method comprising: providing a computer readable medium having at least a first accessible portion and a second encrypted portion" is taught in Ripley col. 4, lines 4-46;

"initializing a password module according to unique data stored within a cryptographic module" is shown in Ripley col. 1, lines 44-46;

the following is not explicitly taught in Ripley:

"transmitting an encrypted password to the cryptographic module; authenticating the encrypted password; decrypting the encrypted password" however Yoshino teaches the

exchange of encrypted keys for authentication between media and the device it is loaded into in col. 34, lines 42-57. Note the Examiner interprets the exchanged key equivalent to passwords.

"transmitting the decrypted password to the computer readable medium; and decrypting the second encrypted portion using the decrypted password" however Yoshino decrypting the content with the decrypted password (i.e. key) in col. 34, lines 58-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and apparatus for verifying the integrity of a media key block taught in Ripley to include a means to transmit encrypted passwords. One of ordinary skill in the art would have been motivated to perform such a modification because a needs exists for assurance of security without increasing processor load see Yoshino (col. 2, lines 42 et seq.) "It is an object of the present invention to provide an information recording device, an information playback device, and an information playback method in which, in the construction of storing data in units of sectors, ICVs are set in units of sectors, without increasing a processing load on a device side. It is also an object of the present invention to provide an information recording medium and a program providing medium which are used therewith".

As to dependent claim 23, "further comprising copying data from a source storage device, and storing the data in the second encrypted portion of the computer readable medium" is taught in Ripley col. 2, lines 54-67.

As to dependent claim 25, "further comprising initializing the password module according to unique data stored within a second cryptographic module" is shown in Ripley col. 1, lines 44-46.

As to dependent claim 26, "further comprising storing and transporting data in the accessible portion of the computer readable medium" is taught in Ripley col. 4, lines 37-46.

As to independent claim 17, this claim is directed to a computer readable storage medium executing the method of claim 22; therefore it is rejected along similar rationale.

As to dependent claims 18, 20, and 21, these claims contain substantially similar subject matter as claims 23, 25, and 26; therefore they are rejected along similar rationale.

As to independent claim 27, this claim is directed to an apparatus executing the method of claim 22; therefore it is rejected along similar rationale.

As to dependent claims 28 and 30, these claims contain substantially similar subject matter as claims 23, 25, and 26; therefore they are rejected along similar rationale.

12. **Claims 19, 24, and 29,** are rejected under 35 U.S.C. 103(a) as being unpatentable over of Ripley U.S. Patent No. 7,111,175 (hereinafter Ripley) in view of Yoshino et al. U.S. Patent No. 7,124,317 (hereinafter Yoshino) in further view of Nonaka et al. U.S. Patent Publication No. 2001/0003517 (hereinafter Nonaka).

As to dependent claim 24, the following is not explicitly taught in Ripley and Yoshino: **"further comprising restoring data to the source storage device from the computer readable medium"** however Nonaka teaches restoring data from a backup on page 1, paragraph 0006.

It would have been obvious to one of ordinary skill in the art at the time of the invention a method and apparatus for verifying the integrity of a media key block that transmits encrypted passwords taught in Ripley and Yoshino to restore data from encrypted backups. One of ordinary skill in the art would have been motivated to perform such a modification because a

needs exists for a user who has purchased digital data to legally save a backup see Nonaka (page 1, paragraph 004) "For example, under the above regulation a user is not allowed to prepare a backup copy for his or her legally obtained one or more of music data, image data and computer program data. As a result, an inconvenience will be unfairly brought about to him or her. Namely, if a user's legally obtained music data, image data or computer program data stored in the HDD (Hard Disc) of his or her personal computer has been accidentally damaged, the user has to again buy the same music data, image data or computer program data. Sometimes, it is even impossible to again obtain the same music data, image data or computer program data (for example, out of stock). In addition, if information data is a computer program, and if the computer program stored in the hard disc of a user's personal computer has become old, it will be impossible to perform a version-up processing on the old computer program".

As to dependent claims 19 and 29, these claims contain substantially similar subject matter as claim 24; therefore they are rejected along similar rationale.

Conclusion

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ellen Tran
Patent Examiner
Technology Center 2134
7 June 2007